312-49 Q&As

ECCouncil Computer Hacking Forensic Investigator (V9)

Pass EC-COUNCIL 312-49 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/312-49.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

![Pass2Lead logo](https://Pass2Lead.com)
QUESTION 1

Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server\'s root directory?

A. Parameter/form tampering

B. Unvalidated input

C. Directory traversal

D. Security misconfiguration

Correct Answer: C

QUESTION 2

UEFI is a specification that defines a software interface between an OS and platform firmware. Where does this interface store information about files present on a disk?

A. BIOS-MBR

B. GUID Partition Table (GPT)

C. Master Boot Record (MBR)

D. BIOS Parameter Block

Correct Answer: B

QUESTION 3

You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other systems?

A. Net sessions

B. Net config

C. Net share

D. Net use

Correct Answer: D

QUESTION 4

While looking through the IIS log file of a web server, you find the following entries:

```
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index.asp
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /login.asp?username=if ((select user)='sa' OR (select user)='dbo')
select 1 else select 1/0
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Developments/index_02.jpg
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index_C4.jpg
```

What is evident from this log file?

A. Web bugs

B. Cross site scripting

C. Hidden fields

D. SQL injection is possible

Correct Answer: D

QUESTION 5

In the following email header, where did the email first originate from?

```
Microsoft Mail Internet Headers Version 2.0
Received: from smtp1.somedomain.com ([199.190.129.133]) by somedomain.com
with Microsoft SMTPSVC(6.0.3790.1830);
        Fri, 1 Jun 2007 09:43:08 -0500
Received: from david1.state.us.gov.us (david1.state.ok.gov [172.16.28.115])
        by smtp1.somedomain.com (8.13.1/8.12.11) with ESMTP id l51EfCEh032241
        for <someone@somedomain.com>; Fri, 1 Jun 2007 09:41:13 -0500
Received: from simon1.state.ok.gov.us ([172.18.0.199]) by
david1.state.ok.gov.us with Microsoft SMTPSVC(6.0.3790.1830);
        Fri, 1 Jun 2007 09:41:13 -0500
X-Ninja-PIM: Scanned by Ninja
X-Ninja-AttachmentFiltering: (no action)
X-MimeOLE: Produced By Microsoft Exchange V6.5.7235.2
Content-class: urn:content-classes:message
Return-Receipt-To: "Johnson, Jimmy" <jimmy@somewherelese.com>
MIME-Version: 1.0
```

A. Somedomain.com

B. Smtp1.somedomain.com

C. Simon1.state.ok.gov.us

D. David1.state.ok.gov.us

Correct Answer: C